UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/613,636	07/03/2003	Bhargava K. Yenduri	SUNMP459	4610

32291 7590 03/05/2007		EXAMINER
MARTINE PENILLA & GENCARELLA, LLP		HOMAYOUNMEHR, FARID
710 LAKEWAY DRIVE		
SUITE 200	ART UNIT	PAPER NUMBER
SUNNYVALE, CA 94085	2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

PTOL-90A (Rev. 10/06)

	Application No.	Applicant(s)
Office Action Summary	10/613,636	YENDURI, BHARGAVA K.
	Examiner	Art Unit	
	Farid Homayounmehr	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _04 December 2006_.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1,3-13,15-25,27-32,34 and 35_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1,3-13,15-25,27-32,34 and 35_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

    1. ☐ Certified copies of the priority documents have been received.

    2. ☐ Certified copies of the priority documents have been received in Application No. _____.

    3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _12/4/2006_.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____ .

DETAILED ACTION

1.   This action is responsive to communications: application, filed 7/3/2003;

amendment filed 12/4/2006.

2.   Claims 1-36 are pending in the case.

Response to Arguments

3.   Applicant's arguments have been fully considered.

3.1.   Applicant argues, " As noted all of the independent claims are defining that the

kernel modules must be verified before loading. Consequently, the teachings of

Rowland do not apply, as Rowland's system allows loading of kernel modules, and it is

not until a later point that they are detected, as noted in Paragraph 149." It is noted that

Applicant interprets the claim limitations to require verification before loading the kernel

modules. However, claim limitations require verification <u>while</u> the kernel modules are

being loaded, and not necessarily before they are loaded. It is also noted that Applicant

interprets Rowland's teachings of detecting Loadable Kernel Modules (LKM) to be

limited to already loaded kernels, and not applicable to kernels being loaded or not

loaded. In other words, per Applicant's view, Rowland does not teach detecting LKMs

before they are loaded or while they are loaded being loaded in real-time. However,

Rowland incorporates teachings of U.S. Patent Application number 09/268084, to

Rowland (see parag. 136), which is now U.S. Patent No. 6,405,318, titled Intrusion

Detection System. In said patent, Rowland clearly recognized the benefits and teaches

an intrusion detection system that works in real-time to detect malicious activity before

they reach the system (see for example col. 2 line 1 to col. 3 line 5). Therefore, Rowland

suggests performing the verification of LKMs before or during loading to the system.

Based on the above discussion, applicant's argument that limitations of claims are not

disclosed or obvious over Rowland is not persuasive.

3.2.   Applicant's argument relative to some elements of dependent claims missing

from Rowland is found persuasive. The mentioned dependent claims are incorporated

into the independent claims as a result of applicant's amendments. See the new

grounds of rejection in the following sections.

Information Disclosure Statement

4.   Information Disclosure Statement submitted by applicant on 12/4/2006 has been

considered. See attached form PTO-1449.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 1, 3-13, 15-25, 27-32, 34 and 35 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Rowland (US Patent Application Publication No. 2002/0129264

A1, filed January 10, 2002).

6.1.   As per claim 1, Rowland is directed to a computer system comprising: a

processor; a memory storage unit; an operating system comprising a kernel, said kernel

comprising a plurality of kernel modules, said kernel modules comprising signature

information; and a kernel module signature verification system for verifying said kernel

module signature information of each of said plurality of kernel modules as said plurality

of kernel modules are loaded into said kernel (paragraph 149 describes a Loadable

Kernel Module Agent 1306, which is an agent looking for loadable kernels and verifies

their validity. As shown in Fig. 13, item 1306 is one of the agents in the group of Mobile

Autonomous Code (MAC) Security Agents. Another one of the MAC agents is Known

Intrusion Agent 1305 (paragraph 148), which uses signatures to identify intrusions such

as suspect loadable kernel modules), wherein said kernel module signature information

is generated via a public key and a private key compilation in said kernel module (use of

public and private keys to create a signature verification protocol is well-known in the

art).

6.2.   Claim 2 has been cancelled by the applicant.

6.3.   As per claims 3 and 4, Rowland is directed to the computer system of claim 1,

wherein said kernel module signature information comprises signature length data

unique to each of said plurality of kernel modules, said signature length or size data

used by said kernel module signature verification system in uniquely identifying each of

said plurality of kernel modules (the signature verification process generates the

signature of data and compares it with the signature. The generated signature and the

signature must be identical, which means the length and size of the generated signature

and the signature must also be identical).

6.4.   As per claim 5, Rowland is directed to the computer system of claim 4, wherein

said kernel module signature verification system comprises a kernel cryptographic

framework for verifying said kernel module signature information (paragraph 132).

6.5.   As per claim 6, Rowland is directed to the computer system of claim 5, wherein

said kernel module signature verification system further comprises a kernel

cryptographic framework daemon for performing verification lookup operations of

signature information provided to said kernel cryptographic framework in said kernel (paragraph 153 shows use of system daemons to run a software process).

6.6.   As per claim 7, Rowland is directed to the computer system of claim 6, wherein said kernel cryptographic framework daemon further performs module verification of said plurality of kernel modules (see response to claim 6).

6.7.   As per claim 8, Rowland is directed to the computer system of claim 7, wherein said kernel cryptographic framework retrieves pathname information of said signature information for each of said plurality of kernel modules when said plurality of kernel modules attempt to load up to said kernel to perform cryptographic operations (retrieving the pathname information is part of a typical access process in a computer. When the signature is fetched from the memory to the cryptographic process, it is accessed by its pathname.)

6.8.   As per claim 9, Rowland is directed to the computer system of claim 8, wherein said kernel cryptographic framework comprises a cryptographic service provider registration unit for registering each of said plurality of kernel modules wishing to provide cryptographic services in said kernel (per paragraph 29, all agents and processes of Rowland register with a module that oversees their operation).

6.9.   As per claim 10, Rowland is directed to the computer system of claim 9, wherein

said kernel cryptographic framework further comprises a intra-kernel communication

unit for enabling communications between said kernel cryptographic framework and

said kernel cryptographic framework daemon (paragraph 29 suggests a Master Control

Process which is a communication unit allowing elements of the system to communicate

with one another.).

6.10.   As per claim 11, Rowland is directed to the computer system of claim 10,

wherein said kernel cryptographic framework further comprises a data structure unit for

storing said kernel module signature information (Rowland agents access to many

different kinds of data, including signature data. Use of datastructures in computer

systems to provide data to processes is well-known in the art).

6.11.   Limitations of claims 12, 13, 15-22, 25, 27-32, and 35 are substantially the same

as claims 1-11 above.

6.12.   As per claim 23, Rowland is directed to the computer operating system of claim

22, wherein said kernel cryptographic framework and said kernel cryptographic

framework daemon communicate via a plurality of input/output control commands

(paragraphs 29-31 describes how handlers communicate with one another to exchange

messages. The messages contain commands to initiate the functionality of each

handler).

6.13. As per claim 24, Rowland is directed to the computer operating system of claim

23, wherein said input/output control commands comprise a door create command for

creating a plurality of cryptographic doors for enabling communication between said

kernel cryptographic framework and said kernel cryptographic framework daemon

(paragraph 87 discloses use of secured messaging between different elements of the

system).

6.14. As per claim 34, Rowland is directed to the method of claim 33, wherein said

kernel cryptographic framework daemon verifies signature data contained in each of

said plurality of kernel cryptographic modules after said requesting kernel module has

registered with said kernel cryptographic framework (Rowland verifies validity of files,

messages and other data using the signature handler (paragraph 124-127). The

signature handler verifies signatures used by the Loadable Kernel Module Agent 1306,

or Known Intrusion Agent 1305 to detect unauthorized Kernel modules).

6.15. Claims 14, 26, 33 and 36 were cancelled by the applicant.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Farid Homayounmehr whose telephone number is 571
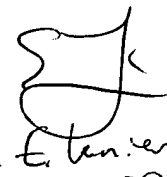
272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday

biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

Examiner

Art Unit: 2132